Publicatieblad
van de Europese Unie

NL
L-serie

2024/2979

4.12.2024

UITVOERINGSVERORDENING (EU) 2024/2979 VAN DE COMMISSIE

van 28 november 2024

tot vaststelling van uitvoeringsbepalingen voor Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad wat betreft de integriteit en de kernfunctionaliteiten van Europese portemonnees voor digitale identiteit

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG ([1]), en met name artikel 5 bis, lid 23,

Overwegende hetgeen volgt:

(1) Het bij Verordening (EU) nr. 910/2014 vastgestelde Europees kader voor digitale identiteit is een cruciaal onderdeel van de totstandbrenging van een veilig en interoperabel ecosysteem voor digitale identiteit in de hele Unie. Met de Europese portemonnee voor digitale identiteit ("de portemonnee") als hoeksteen heeft het kader tot doel de toegang tot diensten in alle lidstaten te vergemakkelijken en de bescherming van persoonsgegevens en de persoonlijke levenssfeer te waarborgen.

(2) Verordening (EU) 2016/679 van het Europees Parlement en de Raad ([2]) en, in voorkomend geval, Richtlijn 2002/58/EG van het Europees Parlement en de Raad ([3]) zijn van toepassing op alle activiteiten betreffende de verwerking van persoonsgegevens uit hoofde van deze verordening.

(3) In artikel 5 bis, lid 23, van Verordening (EU) nr. 910/2014 wordt de Commissie opgedragen om, waar nodig, de relevante specificaties en procedures vast te stellen. Dit wordt bereikt door middel van vier uitvoeringsverordeningen, die betrekking hebben op protocollen en interfaces: Uitvoeringsverordening (EU) 2024/2982 van de Commissie ([4]), op integriteit en kernfunctionaliteiten: Uitvoeringsverordening (EU) 2024/2979 van de Commissie ([5]), op persoonsidentificatiegegevens en elektronische attestering van attributen: Uitvoeringsverordening (EU) 2024/2977 van de Commissie ([6]), en op de kennisgevingen aan de Commissie: Uitvoeringsverordening (EU) 2024/2980 van de Commissie ([7]). In deze verordening worden de relevante vereisten vastgesteld voor de integriteit en kernfunctionaliteiten van de Europese portemonnees voor digitale identiteit.

([1]) PB L 257 van 28.8.2014, blz. 73, ELI: https://eur-lex.europa.eu/eli/reg/2014/910/oj.

([2]) Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PB L 119 van 4.5.2016, blz. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([3]) Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) (PB L 201 van 31.7.2002, blz. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([4]) Uitvoeringsverordening (EU) 2024/2982 van de Commissie van 28 november 2024 tot vaststelling van uitvoeringsbepalingen voor Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad wat betreft de protocollen en interfaces die moeten worden ondersteund door het Europees kader voor digitale identiteit (PB L, 2024/2982, 4.12.2024, ELI: https://data.europa.eu/eli/reg_impl/2024/2982/oj).

([5]) Uitvoeringsverordening (EU) 2024/2979 van de Commissie van 28 november 2024 tot vaststelling van uitvoeringsbepalingen voor Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad wat betreft de integriteit en de kernfunctionaliteiten van Europese portemonnees voor digitale identiteit (PB L, 2024/2979, 4.12.2024, ELI: https://data.europa.eu/eli/reg_impl/2024/2979/oj).

([6]) Uitvoeringsverordening (EU) 2024/2977 van de Commissie van 28 november 2024 tot vaststelling van uitvoeringsbepalingen voor Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad wat betreft de persoonsidentificatiegegevens en elektronische attesteringen van attributen, afgegeven voor de Europese portemonnee voor digitale identiteit (PB L, 2024/2977, 4.12.2024, ELI: https://data.europa.eu/eli/reg_impl/2024/2977/oj).

([7]) Uitvoeringsverordening (EU) 2024/2980 van de Commissie van 28 november 2024 tot vaststelling van uitvoeringsbepalingen voor Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad wat betreft de kennisgevingen aan de Commissie over het ecosysteem van de Europese portemonnee voor digitale identiteit, (PB L, 2024/2980, 4.12.2024, ELI: https://data.europa.eu/eli/reg_impl/2024/2980/oj).

(4) De Commissie voert regelmatig beoordelingen uit van nieuwe technologieën, praktijken, normen of technische specificaties. Om het hoogste niveau van harmonisatie tussen de lidstaten te waarborgen voor de ontwikkeling en de certificering van de portemonnees, berusten de in deze uitvoeringsverordening vastgestelde technische specificaties op de werkzaamheden die zijn verricht op basis van Aanbeveling (EU) 2021/946 van de Commissie van 3 juni 2021 betreffende een gemeenschappelijke EU-toolbox voor een gecoördineerde aanpak ten behoeve van een Europees kader voor digitale identiteit ([8]), en met name de architectuur en het referentiekader. Overeenkomstig overweging 75 van Verordening (EU) 2024/1183 van het Europees Parlement en de Raad ([9]) moet de Commissie deze uitvoeringsverordening in voorkomend geval evalueren en actualiseren om deze in overeenstemming te houden met de mondiale ontwikkelingen, de architectuur en het referentiekader en om de beste praktijken op de interne markt te volgen.

(5) Met het oog op nauwkeurige communicatie, technische differentiatie en een duidelijke verdeling van verantwoordelijkheden moet een onderscheid worden gemaakt tussen de verschillende componenten en configuraties van portemonnees. Een portemonneeoplossing moet worden begrepen als het volledige systeem dat door een portemonneeaanbieder wordt aangeboden en dat nodig is om een portemonnee te exploiteren. Dit moet de software- en hardwarecomponenten omvatten, alsook de diensten, instellingen en configuraties om de portemonnee naar behoren te laten functioneren. Een portemonneeoplossing kan zich bevinden op de apparaten en omgevingen van de gebruikers en op de backend-structuur van de aanbieder. Een portemonnee-eenheid moet worden begrepen als een specifieke configuratie van de portemonneeoplossing voor een individuele gebruiker. Die moet de op het apparaat of de omgeving van een gebruiker van een portemonnee geïnstalleerde toepassing omvatten, waarmee de portemonneegebruiker rechtstreeks interageert (de "portemonnee-instantie") en de beveiligingskenmerken om de gegevens en transacties van de gebruikers te beschermen. Die beveiligingskenmerken moeten speciale software of hardware omvatten om gevoelige informatie te versleutelen en te beveiligen. Een portemonnee-instantie moet deel uitmaken van de portemonnee-eenheid en de portemonneegebruiker toegang geven tot de functionaliteiten van zijn portemonnee.

(6) Beveiligde cryptografische toepassingen voor portemonnees als afzonderlijke gespecialiseerde componenten binnen een portemonnee-eenheid zijn niet alleen noodzakelijk voor de bescherming van kritieke activa, zoals cryptografische privésleutels, maar ook voor het aanbieden van cruciale functionaliteiten, zoals de weergave van elektronische attesteringen van attributen. Het gebruik van gemeenschappelijke technische specificaties kan de toegang tot ingebedde beveiligde elementen door portemonneeaanbieders faciliteren. Beveiligde cryptografische toepassingen voor portemonnees kunnen op verschillende wijzen en aan uiteenlopende beveiligde cryptografische middelen voor portemonnees worden verstrekt. Als aangepaste beveiligde cryptografische toepassingen voor portemonnees door portemonneeaanbieders als Java Card applets aan ingebedde beveiligde elementen worden verstrekt, moeten de portemonneeaanbieders de normen in bijlage I of gelijkwaardige technische specificaties volgen.

(7) Portemonnee-eenheden moeten verstrekkers van persoonsidentificatiegegevens of elektronische attesteringen van attributen in staat stellen te verifiëren of zij deze gegevens of attesteringen afgeven aan echte portemonnee-eenheden van de gebruiker van de portemonnee.

(8) Om gegevensbescherming door ontwerp en door standaardinstellingen te waarborgen, moeten de portemonnees worden voorzien van de meest geavanceerde en geactualiseerde beschikbare privacybevorderende technologie. Die kenmerken moeten de mogelijkheid bieden dat portemonnees kunnen worden gebruikt zonder dat de portemonnee-gebruiker kan worden gevolgd door verschillende op portemonnees vertrouwende partijen, indien van toepassing in het gebruiksscenario. Portemonneeaanbieders moeten bijvoorbeeld overwegen de meest geavanceerde maatregelen voor privacybescherming te nemen met betrekking tot attesteringen voor portemonnee-eenheden, zoals het gebruik van tijdelijke attesteringen voor portemonnee-eenheden of de afgifte van batches. Daarnaast moet het ingebed openbaarmakingsbeleid de portemonneegebruikers waarschuwen tegen ongepaste of illegale openbaarmaking van attributen uit elektronische attesteringen van attributen.

(9) Attesteringen voor portemonnee-eenheden moeten het voor op portemonnees vertrouwende partijen die attributen van portemonnee-eenheden opvragen, mogelijk maken om de geldigheidsstatus te verifiëren van de portemonnee-eenheid waarmee zij communiceren, aangezien attesteringen van een portemonnee-eenheid moeten worden ingetrokken als een portemonnee-eenheid niet langer geldig wordt geacht. De informatie over de geldigheidsstatus van de portemonnee-eenheden moet op interoperabele wijze beschikbaar worden gesteld zodat zij door alle op portemonnees vertrouwende partijen kan worden gebruikt. Bovendien moeten portemonneeaanbieders, in gevallen waarin gebruikers hun portemonnee-eenheid hebben verloren of er geen controle meer over hebben, portemonnee-gebruikers in staat stellen om de intrekking van hun portemonnee-eenheid aan te vragen. Om de privacy en de onkoppelbaarheid te waarborgen, moeten de lidstaten ook voor de portemonnee-eenheidsattestering gebruikmaken van privacybeschermingstechnieken. Dit kan het gebruik van meerdere portemonnee-eenheidsattesteringen voor verschillende doeleinden omvatten, waarbij alleen de minimaal relevante informatie over de portemonnee wordt verstrekt die nodig is voor een transactie, of om de levensduur van de portemonnee-eenheidsattesteringen te beperken als alternatief voor het gebruik van identificatiecodes voor intrekking.

([8]) PB L 210 van 14.6.2021, blz. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj.

([9]) Verordening (EU) 2024/1183 van het Europees Parlement en de Raad van 11 april 2024 tot wijziging van Verordening (EU) nr. 910/2014, wat betreft de vaststelling van het Europees kader voor digitale identiteit (PB L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(10) De portemonnees moeten vooraf bepaalde gegevensformaten en selectieve openbaarmaking ondersteunen zodat ze technisch in staat zijn om persoonsidentificatiegegevens en elektronische attesteringen van attributen in grensoverschrijdende scenario's te ontvangen en weer te geven zonder dat de interoperabiliteit in gevaar komt. Overeenkomstig Verordening (EU) nr. 910/2014 is selectieve openbaarmaking een concept dat de eigenaar van de gegevens toelaat alleen bepaalde delen van een grotere gegevensverzameling openbaar te maken, zodat de ontvangende entiteit alleen die informatie verkrijgt die nodig is voor het verstrekken van een door een gebruiker gevraagde dienst. Aangezien de portemonnees de gebruiker in staat moeten stellen attributen selectief openbaar te maken, moeten de normen in bijlage II zo worden ingevoerd dat de portemonnees die functie ondersteunen. Daarnaast kunnen portemonnees andere formaten en functies ondersteunen om specifieke gebruiksgevallen te vergemakkelijken.

(11) Het registreren van transacties is een belangrijk instrument om de portemonneegebruiker transparantie te bieden in de vorm van een overzicht van de transacties. Voorts moeten logbestanden worden gebruikt om, op verzoek van de gebruiker van de portemonnee, bepaalde informatie snel en gemakkelijk te kunnen delen met de bevoegde toezichthoudende autoriteiten die zijn ingesteld op grond van artikel 51 van Verordening (EU) 2016/679, in geval van verdacht gedrag van op portemonnees vertrouwende partijen.

(12) Om een portemonneegebruiker elektronisch te laten ondertekenen, moet een gekwalificeerd certificaat, dat gebonden is aan een gekwalificeerd middel voor het aanmaken van elektronische handtekeningen, aan de portemonneegebruiker worden afgegeven. De portemonneegebruiker moet toegang hebben tot een toepassing voor het aanmaken van een handtekening. Hoewel de afgifte van gekwalificeerde certificaten een dienst van gekwalificeerde verleners van vertrouwensdiensten is, moeten portemonneeaanbieders of andere entiteiten de andere componenten kunnen leveren. Gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen kunnen bijvoorbeeld door gekwalificeerde verleners van vertrouwensdiensten als dienst worden beheerd of kunnen lokaal staan op het apparaat van de gebruiker van de portemonnee, bijvoorbeeld als een smartcard. Evenzo kunnen toepassingen voor het aanmaken van handtekeningen in de portemonnee-instantie worden geïntegreerd, een afzonderlijke app zijn op het apparaat van de portemonneegebruiker of op afstand worden verstrekt.

(13) Objecten voor gegevensexport en -overdraagbaarheid kunnen de persoonsidentificatiegegevens en elektronische attesteringen registreren van attributen die aan een bepaalde portemonnee-eenheid zijn afgegeven. Deze objecten stellen portemonneegebruikers in staat de relevante gegevens uit hun portemonnee-eenheid te halen, zodat hun recht op gegevensoverdraagbaarheid wordt versterkt. Portemonneeaanbieders worden aangemoedigd om dezelfde technische oplossingen te gebruiken om ook backup- en herstelprocessen voor portemonnee-eenheden in te voeren, zodat verloren portemonnee-eenheden kunnen worden hersteld of informatie van de ene aanbieder van portemonnees naar de andere kan worden overgedragen, voor zover dit mogelijk is zonder afbreuk te doen aan het recht op gegevensbescherming en de beveiliging van het ecosysteem voor digitale identiteit.

(14) Het genereren van specifieke pseudoniemen die betrekking hebben op op portemonnees vertrouwende partijen, moet portemonneegebruikers in staat stellen zich te authenticeren zonder dat zij onnodige informatie verstrekken aan vertrouwende partijen van portemonnees. Overeenkomstig Verordening (EU) nr. 910/2014 mogen gebruikers van de portemonnee niet worden belet om diensten onder een pseudoniem te benaderen, als er geen wettelijke vereisten voor een wettelijke identiteit voor authentificatie bestaat. Daarom moeten de portemonnees een functie bevatten om door de gebruiker gekozen en beheerde pseudoniemen te genereren om zich bij de toegang tot onlinediensten te authenticeren. De uitvoering van de specificaties in bijlage V moet het mogelijk maken die functionaliteit op die manier te gebruiken. Voorts mogen op portemonnees vertrouwende partijen gebruikers niet om andere gegevens verzoeken dan die welke voor het beoogde gebruik van portemonnees in het register van de vertrouwende partij zijn aangegeven. Portemonneegebruikers moeten op elk moment de registratiegegevens van vertrouwende partijen kunnen verifiëren.

(15) Overeenkomstig Verordening (EU) 2024/1183 mogen de lidstaten noch direct, noch indirect de toegang tot publieke of private diensten beperken voor natuurlijke of rechtspersonen die ervoor kiezen geen gebruik te maken van portemonnees, en moeten zij passende alternatieve oplossingen beschikbaar stellen.

(16) De Europese Toezichthouder voor gegevensbescherming is overeenkomstig artikel 42, lid 1, van Verordening (EU) 2018/1725 van het Europees Parlement en de Raad ([10]) geraadpleegd en heeft op 30 september 2024 een advies uitgebracht.

([10]) Verordening (EU) 2018/1725 van het Europees Parlement en de Raad van 23 oktober 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en betreffende het vrije verkeer van die gegevens, en tot intrekking van Verordening (EG) nr. 45/2001 en Besluit nr. 1247/2002/EG (PB L 295 van 21.11.2018, blz. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

(17) De in deze verordening vervatte maatregelen zijn in overeenstemming met het advies van het in artikel 48 van Verordening (EU) nr. 910/2014 bedoelde comité,

HEEFT DE VOLGENDE VERORDENING VASTGESTELD:

HOOFDSTUK I

ALGEMENE BEPALINGEN

Artikel 1

Onderwerp en toepassingsgebied

Bij deze verordening worden regels vastgesteld voor de integriteit en kernfunctionaliteiten van portemonnees, die regelmatig worden bijgewerkt om in overeenstemming te blijven met de ontwikkelingen op het gebied van technologie en normen en met de werkzaamheden die worden verricht op basis van Aanbeveling (EU) 2021/946 van de Commissie, en met name de architectuur en het referentiekader.

Artikel 2

Definities

Voor de doelstellingen van deze verordening, zijn de volgende definities van toepassing:

1) "beveiligde cryptografische toepassing voor portemonnees": een toepassing die kritieke activa beheert door middel van koppeling aan en gebruikmaking van de cryptografische en niet-cryptografische functies van het beveiligd cryptografisch middel voor portemonnees;

2) "portemonnee": een unieke configuratie van een portemonnee-oplossing die bestaat uit portemonnee-instanties, beveiligde cryptografische toepassingen voor portemonnees en beveiligde cryptografische middelen voor portemonnees die door een aanbieder van portemonnees aan een individuele portemonneegebruiker worden verstrekt;

3) "kritieke activa": activa in of met betrekking tot een portemonnee-eenheid die van dermate groot belang zijn dat, als de beschikbaarheid, de authenticiteit of de integriteit ervan in gevaar zou komen, dat een zeer ernstig, verzwakkend effect zou hebben op het vermogen om de portemonnee-eenheid te kunnen gebruiken;

4) "verstrekker van persoonsidentificatiegegevens": een natuurlijke of rechtspersoon die verantwoordelijk is voor de afgifte en de intrekking van persoonsidentificatiegegevens en die ervoor zorgt dat de persoonsidentificatiegegevens van een gebruiker cryptografisch verbonden zijn met een portemonnee-eenheid;

5) "gebruiker van de portemonnee": een gebruiker die de controle heeft over de portemonnee-eenheid;

6) "op portemonnees vertrouwende partij": een vertrouwende partij die voornemens is portemonnee-eenheden te gebruiken voor het verlenen van publieke of private diensten door middel van digitale interactie;

7) "aanbieder van portemonnees": een natuurlijke of rechtspersoon die portemonnee-oplossingen aanbiedt;

8) "portemonnee-eenheidsattestering": een gegevensobject dat de componenten van de portemonnee-eenheid beschrijft en authenticatie en validering van die componenten mogelijk maakt;

9) "ingebed openbaarmakingsbeleid": regels die zijn opgenomen in een elektronische attestering van attributen door de aanbieder ervan, die de voorwaarden aangeeft waaraan een vertrouwende partij moet voldoen om toegang te krijgen tot de elektronische attestering van attributen;

10) "portemonnee-instantie": de toepassing die is geïnstalleerd en geconfigureerd op het apparaat of in de omgeving van een gebruiker van de portemonnee, die deel uitmaakt van een portemonnee-eenheid, en die de portemonnee-gebruiker gebruikt voor de interactie met de portemonnee-eenheid;

11) "portemonnee-oplossing": een combinatie van software, hardware, diensten, instellingen en configuraties, met inbegrip van portemonnee-instanties, een of meer beveiligde cryptografische toepassingen voor portemonnees en een of meer beveiligde cryptografische middelen voor portemonnees;

12) "beveiligd cryptografisch middel voor portemonnees": een manipulatiebestendig apparaat dat een omgeving biedt die gekoppeld is aan en wordt gebruikt door de beveiligde cryptografische toepassing voor portemonnees om kritieke activa te beschermen en cryptografische functies te bieden voor de veilige uitvoering van kritieke activiteiten;

13) “cryptografische bewerking van portemonnees”: een cryptografisch mechanisme dat nodig is in het kader van de authenticatie van de portemonneegebruiker en de afgifte of weergave van persoonsidentificatiegegevens of elektronische attesteringen van attributen;

14) “toegangscertificaat voor een op portemonnees vertrouwende partij”: een certificaat voor elektronische zegels of handtekeningen ter authenticatie en validering van de op portemonnees vertrouwende partij, afgegeven door een aanbieder van toegangscertificaten voor op portemonnees vertrouwende partijen;

15) “aanbieder van toegangscertificaten voor op portemonnees vertrouwende partijen”: een natuurlijke of rechtspersoon die door een lidstaat is gemachtigd om toegangscertificaten voor op portemonnees vertrouwende partijen af te geven aan in die lidstaat geregistreerde op portemonnees vertrouwende partijen.

HOOFDSTUK II

INTEGRITEIT VAN EUROPESE PORTEMONNEES VOOR DIGITALE IDENTITEIT

Artikel 3

Integriteit van de portemonnee-eenheid

1. Portemonnee-eenheden mogen geen van de in artikel 5 bis, lid 4, van Verordening (EU) nr. 910/2014 vermelde functies uitvoeren, met uitzondering van authenticatie van de portemonneegebruiker om toegang tot de portemonnee-eenheid te krijgen, totdat de portemonnee-eenheid de portemonneegebruiker met succes heeft geauthenticeerd.

2. Portemonneeaanbieders ondertekenen of verzegelen voor elke portemonnee-eenheid ten minste één portemonnee-eenheidsattestering die aan de vereisten van artikel 6 voldoet. Het certificaat dat wordt gebruikt om de portemonnee-eenheidsattestering te ondertekenen of te verzegelen, wordt afgegeven op basis van een certificaat dat is opgenomen in de vertrouwenslijst als bedoeld in Uitvoeringsverordening (EU) 2024/2980.

Artikel 4

Portemonnee-instanties

1. Portemonnee-instanties gebruiken ten minste één beveiligd cryptografisch middel voor portemonnees voor het beheer van kritieke activa.

2. Portemonneeaanbieders waarborgen de integriteit, de authenticiteit en de vertrouwelijkheid van de communicatie tussen portemonnee-instanties en de beveiligde cryptografische toepassingen voor portemonnees.

3. Wanneer kritieke activa verband houden met de uitvoering van elektronische identificatie op het betrouwbaarheidsniveau “hoog”, worden de cryptografische bewerkingen van de portemonnee of andere bewerkingen waarbij kritieke activa worden gebruikt, uitgevoerd overeenkomstig de vereisten voor de kenmerken en het ontwerp van elektronische identificatiemiddelen op het betrouwbaarheidsniveau “hoog” in de zin van Uitvoeringsverordening (EU) 2015/1502 van de Commissie ([11]).

Artikel 5

Beveiligde cryptografische toepassingen voor portemonnees

1. Portemonneeaanbieders zorgen ervoor dat beveiligde cryptografische toepassingen voor portemonnees:

a) cryptografische bewerkingen van portemonnees uitsluitend in gevallen waarin die toepassingen met succes gebruikers van portemonnees hebben geauthenticeerd, uitvoeren met andere kritieke activa dan die welke de portemonnee-eenheid nodig heeft om de portemonneegebruiker te authenticeren;

([11]) Uitvoeringsverordening (EU) 2015/1502 van de Commissie van 8 september 2015 tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen overeenkomstig artikel 8, lid 3, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt (PB L 235 van 9.9.2015, blz. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

b) indien zij portemonneegebruikers authenticeren in het kader van de uitvoering van elektronische identificatie op het betrouwbaarheidsniveau "hoog"; de authenticatie van portemonneegebruikers uitvoeren overeenkomstig de voorschriften voor de kenmerken en het ontwerp van elektronische identificatiemiddelen op het betrouwbaarheidsniveau "hoog" in de zin van Uitvoeringsverordening (EU) 2015/1502;

c) veilig nieuwe cryptografische sleutels kunnen genereren;

d) kritieke activa veilig kunnen wissen;

e) een bewijs van het bezit van privésleutels kunnen genereren;

f) de door die beveiligde cryptografische toepassingen voor portemonnees gegenereerde privésleutels beschermen zo lang die sleutels bestaan;

g) voldoen aan de voorschriften voor de kenmerken en het ontwerp van elektronische identificatiemiddelen op het betrouwbaarheidsniveau "hoog" in de zin van Uitvoeringsverordening (EU) 2015/1502;

h) de enige componenten zijn die cryptografische bewerkingen voor portemonnees en alle andere bewerkingen met kritieke activa in het kader van de uitvoering van elektronische identificatie op het betrouwbaarheidsniveau "hoog" kunnen uitvoeren.

2. Als portemonneeaanbieders besluiten een beveiligde cryptografische toepassing aan een ingebed beveiligd element te verstrekken, baseren zij hun technische oplossing op de technische specificaties in bijlage I of andere gelijkwaardige technische specificaties.

Artikel 6

Authenticiteit en geldigheid van de portemonnee-eenheid

1. Portemonneeaanbieders zorgen ervoor dat elke portemonnee-eenheid portemonnee-eenheidsattesteringen bevat.

2. Portemonneeaanbieders zorgen ervoor dat de in lid 1 bedoelde portemonnee-eenheidsattesteringen openbare sleutels bevatten en dat de overeenkomstige privésleutels worden beschermd door een beveiligd cryptografisch middel voor portemonnees.

3. Portemonneeaanbieders:

a) informeren portemonneegebruikers over hun rechten en plichten met betrekking tot hun portemonnee-eenheid;

b) verstrekken mechanismen, onafhankelijk van de portemonnee-eenheden, voor de veilige identificatie en authenticatie van gebruikers van de portemonnee;

c) zorgen ervoor dat gebruikers van de portemonnee het recht hebben om te verzoeken om intrekking van hun portemonnee-eenheidsattesteringen, met behulp van de in punt b) bedoelde authenticatiemechanismen.

Artikel 7

Intrekking van portemonnee-eenheidsattesteringen

1. Alleen portemonneeaanbieders mogen de entiteiten zijn die portemonnee-eenheidsattesteringen voor door hen verstrekte portemonnees kunnen intrekken.

2. Portemonneeaanbieders stellen een openbaar beschikbaar beleid vast waarin de voorwaarden en het tijdschema voor de intrekking van portemonnee-eenheidsattesteringen worden gespecificeerd.

3. Wanneer portemonneeaanbieders portemonnee-eenheidsattesteringen hebben ingetrokken, stellen zij de betrokken portemonneegebruikers binnen 24 uur in kennis van de intrekking van hun portemonnee-eenheden, met vermelding van de reden voor de intrekking en de gevolgen voor de gebruiker van de portemonnee. Deze informatie wordt op beknopte, gemakkelijk toegankelijke wijze en in duidelijke en eenvoudige taal verstrekt.

4. Wanneer portemonneeaanbieders portemonnee-eenheidsattesteringen hebben ingetrokken, maken zij de geldigheidsstatus van de portemonnee-eenheidsattestering op een privacybeschermende wijze openbaar en beschrijven ze de locatie van die informatie in de attestering voor de portemonnee-eenheid.

HOOFDSTUK III

KERNFUNCTIONALITEITEN EN -KENMERKEN VAN EUROPESE PORTEMONNEES VOOR DIGITALE IDENTITEIT

Artikel 8

Formaten van persoonsidentificatiegegevens en elektronische attesteringen van attributen

Portemonneeaanbieders zorgen ervoor dat portemonnee-oplossingen het gebruik van persoonsidentificatiegegevens en elektronische attesteringen van attributen die zijn afgegeven in overeenstemming met de lijst van normen in bijlage II, ondersteunen.

Artikel 9

Transactielogboeken

1. Ongeacht of een transactie al dan niet met succes is afgerond, leggen de portemonnee-instantie alle transacties met de op portemonnees vertrouwende partijen en andere portemonnee-eenheden vast, met inbegrip van elektronische ondertekening en verzegeling.

2. De vastgelegde informatie bestaat ten minste uit:

a) het tijdstip en de datum van de transactie;

b) de namen van de contactpersonen en de unieke identificatiecode van de overeenkomstige vertrouwende partij en de lidstaat waar die vertrouwende partij is gevestigd, of, in het geval van andere portemonnee-eenheden, relevante informatie uit de attestering voor de portemonnee;

c) de soort of soorten gegevens die bij de transactie worden opgevraagd en weergegeven;

d) in het geval van niet-voltooide transacties, de reden voor die niet-voltooiing.

3. Portemonneeaanbieders waarborgen de integriteit, de authenticiteit en de vertrouwelijkheid van de vastgelegde informatie.

4. Portemonnee-instanties leggen de meldingen vast die de portemonneegebruiker via de portemonnee-eenheid naar de gegevensbeschermingsautoriteiten stuurt.

5. De in de leden 1 en 2 bedoelde logbestanden zijn op basis van uitdrukkelijke voorafgaande toestemming van de gebruiker van de portemonnee toegankelijk voor de aanbieder van portemonnees, indien dat nodig is voor de levering van portemonneediensten.

6. De in de leden 1 en 2 bedoelde logbestanden blijven toegankelijk zo lang op grond van het Unierecht of het nationale recht vereist is.

7. Portemonneeaanbieders stellen gebruikers van de portemonnee in staat de in lid 2 bedoelde vastgelegde informatie te exporteren.

Artikel 10

Ingebed openbaarmakingsbeleid

1. Portemonneeaanbieders zorgen ervoor dat elektronische attesteringen van attributen met een gemeenschappelijk ingebed openbaarmakingsbeleid als bedoeld in bijlage III kunnen worden verwerkt door de portemonnee-eenheden die zij aanbieden.

2. De portemonnee-instanties moeten in staat zijn dergelijk ingebed openbaarmakingsbeleid als bedoeld in lid 1 te verwerken en weer te geven in samenhang met gegevens die zijn ontvangen van de vertrouwende partij die het verzoek heeft ingediend.

3. De portemonnee-instanties gaan na of de vertrouwende partij voldoet aan de vereisten van het ingebed openbaarmakingsbeleid en de portemonneegebruiker in kennis stellen van het resultaat.

Artikel 11

Gekwalificeerde elektronische handtekeningen en zegels

1. Portemonneeaanbieders zorgen ervoor dat portemonneegebruikers gekwalificeerde certificaten kunnen ontvangen voor gekwalificeerde elektronische handtekeningen of zegels die gekoppeld zijn aan gekwalificeerde middelen voor het aanmaken van handtekeningen of zegels die zich lokaal, extern of op afstand van de portemonnee-instanties bevinden.

2. Portemonneeaanbieders zorgen ervoor dat portemonnee-oplossingen veilig kunnen communiceren met een van de volgende soorten gekwalificeerde middelen voor het aanmaken van handtekeningen of zegels: lokale, externe of op afstand beheerde gekwalificeerde middelen voor het aanmaken van handtekeningen of zegels met het oog op het gebruik van de in lid 1 bedoelde gekwalificeerde certificaten.

3. Portemonneeaanbieders zorgen ervoor dat gebruikers van de portemonnee die natuurlijke personen zijn, ten minste voor niet-professionele doeleinden, gratis toegang hebben tot toepassingen voor het aanmaken van handtekeningen waarmee kosteloos gekwalificeerde elektronische handtekeningen kunnen worden aangemaakt met behulp van de in lid 1 bedoelde certificaten.

Artikel 12

Toepassingen voor het aanmaken van handtekeningen

1. De toepassingen voor het aanmaken van handtekeningen die door portemonnee-eenheden worden gebruikt, kunnen door portemonneeaanbieders, door verleners van vertrouwensdiensten of door op portemonnees vertrouwende partijen worden verstrekt.

2. Toepassingen voor het aanmaken van handtekeningen beschikken over de volgende functies:

a) ondertekenen of verzegelen van door de portemonneegebruiker verstrekte gegevens;

b) ondertekenen of verzegelen van door de vertrouwende partij verstrekte gegevens;

c) creëren van handtekeningen of zegels overeenkomstig ten minste de in bijlage IV bedoelde verplichte formaten;

d) informeren van portemonneegebruikers over het resultaat van het aanmaken van een handtekening of zegel.

3. De toepassingen voor het aanmaken van handtekeningen kunnen in de portemonnee-instanties worden geïntegreerd of extern zijn. Wanneer toepassingen voor het aanmaken van handtekeningen berusten op gekwalificeerde middelen voor het aanmaken van handtekeningen op afstand en wanneer zij in portemonnee-instanties zijn geïntegreerd, ondersteunen zij de in bijlage IV bedoelde applicatieprogramma-interface.

Artikel 13

Gegevensexport en -overdraagbaarheid

Portemonnee-eenheden ondersteunen, indien technisch haalbaar en met uitzondering van kritieke activa, de veilige export en overdraagbaarheid van persoonsgegevens van de gebruiker van de portemonnee, om de gebruiker van de portemonnee in staat te stellen naar een portemonnee-eenheid van een andere portemonnee-oplossing te migreren, met waarborg van een hoog betrouwbaarheidsniveau overeenkomstig Uitvoeringsverordening (EU) 2015/1502.

Artikel 14

Pseudoniemen

1. Portemonnee-eenheden ondersteunen het genereren van pseudoniemen voor portemonneegebruikers overeenkomstig de technische specificaties van bijlage V.

2. Portemonnee-eenheden ondersteunen het genereren, op verzoek van een vertrouwende partij, van een pseudoniem dat specifiek en uniek is voor die vertrouwende partij en verstrekken dit pseudoniem aan de vertrouwende partij, afzonderlijk of in combinatie met de persoonsidentificatiegegevens of de elektronische attestering van attributen waar die op portemonnees vertrouwende partij om verzoekt.

HOOFDSTUK IV

SLOTBEPALINGEN

Artikel 15

Inwerkingtreding

Deze verordening treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te Brussel, 28 november 2024.

Voor de Commissie
De voorzitter
Ursula VON DER LEYEN

BIJLAGE I

LIJST VAN NORMEN ALS BEDOELD IN ARTIKEL 5

— SAM.01 Secured Applications for Mobile — Requirements for supporting 3rd party Applets on eSIM and eSE via SAM. v1.1 2023, GSMA;

— GPC_GUI_ 217 GlobalPlatform SAM Configuration Technical specification for implementation of SAM v1.0 2024-04;

— GPC_SPE_0 34 GlobalPlatform Card Specification Technical specification for smart cards v2.3.1 2018-03;

— GPC_SPE_0 07 GlobalPlatform Amendment A Confidential Card Content Management v1.2 2019-07;

— GPC_SPE_0 13 GlobalPlatform Amendment D Secure Channel Protocol 03 v1.2 2020-04;

— GPC_SPE_0 93 GlobalPlatform Amendment F Secure Channel Protocol 11 v1.4 2024-03;

— GPD_SPE_0 75 Open Mobile API Specification OMAPI API for mobile apps to access secure elements on user devices. v3.3 2018-08, GlobalPlatform.

BIJLAGE II

LIJST VAN NORMEN ALS BEDOELD IN ARTIKEL 8

— ISO/IEC.18013-5:2021;

— “Verifiable Credentials Data Model 1.1” uit de W3C-aanbeveling van 3 maart 2022.

BIJLAGE III

GEMEENSCHAPPELIJK INGEBED OPENBAARMAKINGSBELEID ALS BEDOELD IN ARTIKEL 10

1. "Geen beleid": er is geen beleid van toepassing op de elektronische attesteringen van attributen.
2. "Beleid inzake geautoriseerde vertrouwende partijen": portemonneegebruikers mogen elektronische attestering van attributen alleen openbaar maken aan geauthenticeerde vertrouwende partijen die uitdrukkelijk in het openbaarmakingsbeleid zijn vermeld.
3. "Specifieke bron van vertrouwen": portemonneegebruikers mogen de specifieke elektronische attestering van attributen alleen openbaar maken aan geauthenticeerde op portemonnees vertrouwende partijen met een toegangscertificaat voor op portemonnees vertrouwende partijen die is afgeleid van een specifieke bron (of lijst van specifieke bronnen) of tussenliggend(e) certifica(a)t(en).

BIJLAGE IV

FORMATEN VAN HANDTEKENINGEN EN ZEGELS ALS BEDOELD IN ARTIKEL 12

1. Verplicht formaat voor handtekeningen of zegels:

   a) PAdES (PDF Advanced Electronic Signature), zoals gespecificeerd in ETSI EN 319 142-1, V1.1.1 (2016-04); Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Deel 1: Building blocks and PAdES baseline signatures.

2. Lijst van facultatieve formaten voor handtekeningen of zegels:

   a) XAdES, zoals gespecificeerd in ETSI EN 319 132-1 V1.2.1 (2022-02) Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Deel 1: Building blocks and XAdES baseline signatures (XAdES), voor ondertekening van het XML-formaat;

   b) JAdES, zoals gespecificeerd in ETSI TS 119 182-1 V1.2.1 (2024-07) Electronic Signatures and Infrastructures (ESI); JAdES digital signatures; Deel 1: Building blocks and JAdES baseline signatures, voor ondertekening van het JSON-formaat;

   c) CAdES (CMS Advanced Electronic Signature), zoals gespecificeerd in ETSI EN 319 122-1, V1.3.1 (2023-06): Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Deel 1: Building blocks and CAdES baseline signatures, voor ondertekening van het CMS-formaat;

   d) ASiC (Associated Signature Container) zoals gespecificeerd in ETSI EN 319 162-1, v1.1.1 (2016-04) Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Deel 1: Building blocks and ASiC baseline containers en ETSI EN 319 162-2 V1.1.1 (2016-04) Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Deel 2: Extra ASiC containers voor de ondertekening van containers.

3. Applicatieprogramma-interface:

   — specificatie v2.0 van het Cloud Signature Consortium (CSC) (20 april 2023).

BIJLAGE V

TECHNISCHE SPECIFICATIES VOOR HET GENEREREN VAN PSEUDONIEMEN ALS BEDOELD IN ARTIKEL 14

Technische specificaties:

— WebAuthn: W3C-aanbeveling van 8 april 2021, niveau 2, https://www.w3.org/TR/2021/REC-webauthn-2-20210408/.